**REMARKS**

The present amendment is responsive to the Office Action dated December 20, 2005. Claims 1-6, 8-9, 12-16, 19 and 22-29 have been amended. No new matter has been introduced by these amendments. Claims 1-29 are again presented for the Examiner's consideration in view of the following comments. A petition for a one-month extension of time is respectfully submitted herewith.

Claim 2 was objected to because of a typographical error and claims 1-29 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite due to antecedent basis questions in claims 1, 2, 4, 5, 13, 14, 15, 19, 23, 24 and 29. The claims have been amended to correct the typographical error and antecedent basis questions. With regard to the typographical error of claim 2, this claim now recites "lower rank key" instead of "lower ran key." Claims 1, 2, 4, 5, 14, 15, 19, 23, 24 and 29 have also been amended to address the identified antecedent basis questions. Please note that the preamble of original claim 13 states "...for ciphering a contents data in a storage device as a header data corresponding to said contents data..." Applicants submit that there is sufficient antecedent basis for the recitation of "said contents data" in claim 13. All of the identified typographical and antecedent basis questions having been addressed, applicants respectfully request that the objections and § 112 rejections be withdrawn.

Independent claims 1, 13, 19 and 29 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,832,319 to *Bell et al.* ("the '319 patent"). Applicants respectfully traverse the rejection.

As amended, claim 1 recites "A data processing system which initially stores a contents ciphering key applicable to a contents ciphering process as a header data corresponding to

contents data and then executes a process for ciphering the corresponding contents data by applying said contents ciphering key contained in said header data; wherein said header data comprises a plurality of ciphered contents ciphering keys generated by said contents ciphering key respectively ciphered by applying mutually different key ciphering keys."

Amended claim 13 recites "A method of processing data comprising: an initial step of storing a plurality of contents ciphering keys usable for ciphering a contents data in a storage device as a header data corresponding to said contents data; and an ensuing step of ciphering the corresponding contents data by applying one of said contents ciphering keys present in said header data, wherein: said header data is stored in said storage device, and said header data includes a plurality of ciphered contents ciphering keys generated via a process for ciphering said contents ciphering keys by applying mutually different key ciphering keys."

Amended claim 19 recites "A data processing apparatus for executing recording or reproduction of contents data comprising: a system for initially storing a contents key usable for ciphering a contents data to be stored in a storage device into said storage device as a header data corresponding to said contents data followed by a step of ciphering said contents data by applying said contents key present in said header data; wherein said data processing apparatus further executes a process for storing such header data including a plurality of ciphered contents keys individually ciphered by mutually different key enciphering keys into said storage device."

Amended claim 29 recites "A program providing medium which enables a plurality of contents ciphering keys usable for ciphering contents data to be stored in a storage device as header data corresponding to contents data, and yet, provides a computer program which enables a process for ciphering

corresponding contents data to be executed on a computer system by applying said contents ciphering key present in said header data; wherein said computer program comprises: a step of ciphering said contents ciphering keys by applying mutually different key enciphering keys; and a step of enabling said header data including a plurality of ciphered contents ciphering keys generated via said ciphering step."

The Office Action states that all of the elements of the independent claims are found in the '319 patent. Specifically, the Office Action refers to column 2, lines 52-65 of the '319 patent. This portion of the '319 patent states:

> Also, the present method acts include combining the media key with the media identification to render a content key, and then encrypting the data using the content key for copying of the encrypted data onto a data storage medium.
>
> Preferably, a player-recorder establishes a player and a recorder, and the player-recorder undertakes method acts including sending encrypted data from the data storage medium to the player. The media identification and media key block on the data storage medium are read by the player. Then, the media key is determined using the media key block, and the content key determined using the media key and the media identification. With the content key, the player decrypts the data to facilitate the player playing video and/or audio represented by the data.

According to the '319 patent, "a media identification 34 and a media key block 36 [] are written onto the disk 32 during manufacture by a media manufacturing machine 38." (Col. 6, ll. 20-21. "In accordance with the present invention, the media key block 36 is the same for a large batch of disks 32, which periodically can be changed for a subsequently manufactured batch of disks to combat attacks as discussed further below. In contrast, each disk 32 includes a media identification 34 that is unique to the disk 32, or substantially so. By 'substantially unique' media identification means that actual media identifications can be as little as

sixteen bits long, so that occasionally two randomly selected blank disks might have the same media identification." (Col. 6, ll. 38-47.) The media identification "is preferably written to a read-only area" of the disk 32. (Col. 6, ll. 27-30.)

The Office Action states "the content key [of the '319 patent] is equivalent to the contents ciphering key and processes are equivalent to the instant case." (Office Action, numbered paragraph 8, pg. 5, emphasis added.) Applicants respectfully disagree.

According to the '319 patent, "the recorder combines the media key with the media identification of the disk 32 to which the data is to be copied" in order to generate a content key. Then, "the content key is 'used' to encrypt the data at block 48, which is then recorded onto a blank disk 32." (Col. 6, line 60 to col. 7, line 4; *see also* FIG. 5.)

However, this is not what is claimed in the independent claims. For instance, independent claim 1 requires "header data corresponding to contents data," and that the header data comprise "a plurality of ciphered contents ciphering keys generated by said contents ciphering key respectively ciphered by applying a mutually different key ciphering key." Independent claim 13 requires that the header data include "a plurality of ciphered contents ciphering keys generated via a process for ciphering said contents ciphering keys by applying mutually different key ciphering keys." Independent claims 19 and 29 recite similar limitations. The '319 patent simply does not teach or suggest such limitations.

Thus, for at least the aforementioned reasons, applicants respectfully submit that independent claims 1, 13, 19 and 29 are in condition for allowance.

Claims 2-12, 14-18 and 20-28 were rejected under 35 U.S.C. § 103(a) as being obvious over the '319 patent in view of U.S. Patent No. 6,049,878 to *Caronni et al.* ("the '878 patent").

Claims 2-12, 14-18 and 20-28 depend from independent claims 1, 13 and 19, and contain all of the limitations thereof. Accordingly, for at least this reason, applicants submit that the subject dependent claims are likewise patentable.

As it is believed that all of the rejections set forth in the Office Action have been fully met, favorable reconsideration and allowance are earnestly solicited.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have. If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: April 17, 2006

Respectfully submitted,

By _____

Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

644611_1.DOC